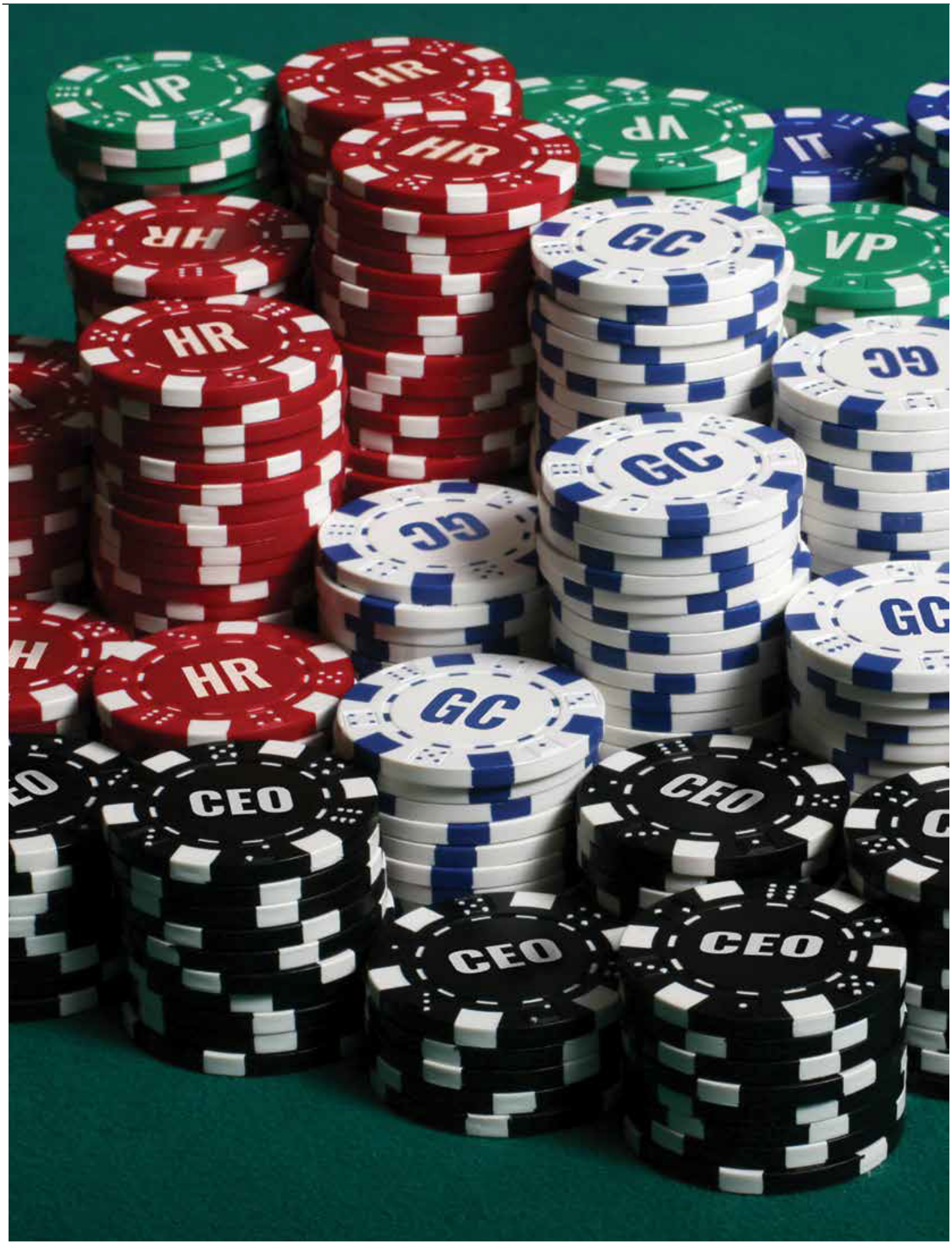
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Compliance & Risk Management in Small Law Departments

Compliance and Ethics


VP
HR
HR
VP
IT
HR
GC
VP
HR
GC
GC
GC
GC
HR
GC
CEO
CEO
CEO
CEO


VP
HR
HR
VP
IT
HR
GC
VP
HR
GC
GC
GC
GC
HR
GC
CEO
CEO
CEO
CEO

CHEAT SHEET

- ***Commit to protect.*** Ensure that that the C-suite is outwardly supportive of creating and honoring new compliance initiatives. This will set the tone for the entire organization.
- ***Spring cleaning.*** In-house counsel should perform a thorough due diligence of old compliance policies to determine what needs to be revised. In doing so, the company will have a clearer understanding of the probability of a compliance violation.
- ***Education dedication.*** Consider how your compliance training measures are implemented and guarantee that each employee receives the same message. This mitigates the risk of misunderstanding.
- ***Using the whistle.*** Be sure that the proper channels exist to report compliance violations. These include confidential email, internet, and telephone “tip lines.”

In many legal departments, particularly with those that qualify as “small,” the notion of devoting one’s already scarce resources to designing, implementing, and monitoring a wholesale compliance program can be horribly intimidating. But more than overwhelming, it is also seemingly a luxury rather than a necessity in an environment where legal departments are often being asked to do far more with less.

Perhaps it was a luxury — five or 10 years ago. But in today’s regulatory climate, developing and curating an effective compliance program is of the utmost importance for all companies (and accordingly, all in-house legal departments). Historically, and for smaller companies in particular, the cost to create a full-scale compliance program in exchange for a potential reduction in penalties is too high to justify the certain investment. To many executives, payments for compliance penalties are simply “the cost of doing business.” Accordingly, US federal agencies have adjusted their own strategies to appeal to that very attitude via levying increased penalties, including, in some cases, personal liability. By increasing what’s at stake for the company and the individuals running it, these agencies hope to tip the cost-benefit analysis away from strategic noncompliance and in favor of falling in line with regulatory requirements.

Regardless of where your company’s compliance efforts exist in the world, whether you’re reading this in Sydney or Seattle, or whether your program is newly-minted or well-traveled, much research and many discussions with in-house lawyers have proven one indelible truth: Nobody has reached the mountaintop. Not even those sitting in the most prestigious of legal departments have found the secret formula for a perfect program. All programs can, and should, be built upon or tailored to more effectively enforce compliance obligations.

Consider the structure of your program — who owns it? Where does it reside? Who is responsible? How is it managed? Each of these questions is every bit as important as the composition of the substance of the program itself. Further, as you read this article and consider how to structure or improve your program, harken back on your elementary school investigatory skills — address the who, what, when, where, why, and how of your program while evaluating your compliance needs.

We’ll start with an easy one: who has assigned the task of creating or modifying your program? Is the initiative one that’s rooted in legal concerns over business practices? Is it the result of the board

or executive management's attempt to better quantify the veritable black hole of liability lurking behind known or presumed non-compliance? Perhaps it's a more urgent effort being forced upon you by a government agency in response to an alleged violation. The source of the compliance push will provide much of the structure and focus of your program.

Who will be responsible for the program? While the lawyers are undeniably qualified as experts in the category of reading, much research has determined that most of the other departments in your company share this gift. Don't be afraid to exploit it. If not outright owners of the program, these other departments should at least be card-carrying members of the club, with their own dues to pay and meetings to attend. The legal department tends to only touch matters in one of three scenarios — either as they come in, as they terminate, or as problems arise. What legal isn't involved in nearly as often is the ordinary conduct of the business. Operations, on the other hand, touch virtually every aspect of what is needed for your company to perform and deliver on a daily basis. Not only will they have the knowledge of what is happening, but also why things happen the way they do. Accordingly, it is vitally important that they play a role in identifying compliance issues and creating necessary real world solutions.

That's not to say that legal shouldn't play a role as well — the lawyers certainly have a broader perspective on many of the regulatory pressures facing the company. Because of this, it makes sense that the legal department have a seat at the table, perhaps even at the head, particularly while the program is under construction. However, as easy as it might be to anoint legal as the architects of the program, the reality is that it will take many different skill sets to keep an effective program spinning.

How are you going to implement or improve your program? Start with guidance issued by the various sources of the regulations inspiring your program, in whichever jurisdictions apply. After all, these regulators will be the ones ultimately grading your compliance efforts. Any insight they provide regarding the rubric for their evaluation should be used as a road map.

For example, the European Union maintains its own export standards through the European Code of Export Compliance, as a means to "encourage the dissemination of best practices and principles in Export Compliance Management" for all EU and non-EU actors involved in the import and export of goods and services. In the United Kingdom, a guide to compliance with the oft-discussed UK Data Protection Act 1998 is maintained by the Information Commissioner's Office, the authority charged with upholding information rights on behalf of the public. Other jurisdictions where your company does business have issued their own compliance best practices, so look to the entities governing your operations for guidance.

Export compliance standards in the European Union

In the European Union, a useful checklist has been enumerated related to Export Compliance Standards. The "10 EU Export Compliance Key Elements" reflect very similar tenets to those laid out in the Ten Hallmarks, and although not identical, there is significant overlap. Despite the fact that the checklist is directed at addressing compliance with specific regulations, either the US or UK guidance cited here would serve as a helpful guide in putting together an effective compliance program. ISO Standards, specifically those set forth in AS/ISO 19600:2015, are another source. Although we focus on the US-based guidance in this article, much of what is referenced here could bear on operations anywhere in the world — the underlying concepts, if reflected in your program, will create the framework for an effort no matter the jurisdiction.

In the United States, the US Department of Justice (DOJ) has published compliance parameters as a part of the Federal Sentencing Guidelines. Additionally, the DOJ and the US Securities and Exchange Commission have issued joint guidance regarding enforcement actions under the US Foreign Corrupt Practices Act. Included in this joint guidance are the aptly-named "Ten Hallmarks of an Effective Compliance Program," put forth in an effort "to provide businesses and individuals with information to help them abide by the law, detect and prevent FCPA violations, and implement effective compliance programs."

As a note, although this guidance is specifically geared toward FCPA compliance in the United States, the underlying characteristics described in these Ten Hallmarks have been widely lauded as indicative of a successful compliance program. Regardless of the jurisdiction in which you operate, if your compliance efforts reflect the concepts set forth in the Ten Hallmarks, you will likely retain a stout defensible position if regulators should come calling. This defensible position may provide some comfort in the form of cooperation credit or reduced fines or penalties.

We'll discuss each of the hallmarks below. The concepts shouldn't be new to many of you, so in that vein we're going to approach them from the standpoint of who within your company can help you realize them. As you review, note that the truly legal responsibilities are somewhat few and far between. Virtually all of them are not specifically driven by the legal team, but rather, are merely supported by lawyers.

Commitment by your organization.

Start with the C-suite. Be sure that the "tone at the top" is one of support and endorsement of your compliance initiatives and fosters a company-wide environment of acceptance. Depending on who is driving the motivation behind structuring or revamping your program, this may be less of an issue. In effort to cut off arguments that compliance is simply another soft cost that does not directly contribute positively to the bottom line, collect research on the increased fines and the potential for personal liability that have become part of the regulatory arsenal. No matter how resistant an executive may be, personal liability can be a useful tool in manufacturing change.

You'll likely be spending your own political capital to implement a program, so make it worthwhile. The commitment you seek should include the assets necessary to make it successful — and be sure that "assets" include both financial and human resources. Give the compliance team its own identity, including a budget. This will be vital to recruiting your team, as no one will want to play if they must also pay a membership fee from their own purse.

Assuming you receive a thorough endorsement, the next step is to turn to the actual implementation of the program — which should involve IT as early as possible. Compliance records should not be commingled in the legal files or sprinkled throughout various departments across the organization. Instead, these may be stored in a shared folder with permissions granted to those on the compliance team who need access. The compliance-based records will need to be managed in a manner appropriate to withstand a discovery event. Records retention rules should be considered and set for the compliance team as though it were its own department.

Consider creating a dedicated email address for the individuals participating in a compliance capacity, as well as another shared email address to use to deliver company-wide messages from

the team. The resulting email content should be managed by the team members in the joint file and in accordance with the records retention structure.

Support staff can also be utilized in the setup of the compliance team to help alleviate the burden on the lawyers, whether by managing records retention, calendaring, and keeping minutes and other records related to compliance meetings, etc. Undertake efforts to limit the compliance exposure from spilling over into other administrative functions for the legal department and traditional legal work.

Meetings of the compliance team should occur at a regular frequency, often enough to satisfy the appetite of those driving compliance efforts. Prior to scheduled board meetings, in-house counsel should compile regulatory filings, year-end close outs of company accounting, and budgeting efforts to be able to respond to the oversight of regulators.

Continuous endorsement of the compliance message is imperative, even if the message is ghost-written by the legal department. It should be clearly articulated and communicated unambiguously by management at all levels at every possible turn. Your managers should be your model citizens, scrupulously following internal compliance policies to the letter.

Regarding delivery of the message of compliance, talk with IT and corporate communications/marketing about the creation of an independently dedicated intranet page for the compliance team. This can be an excellent avenue to share noteworthy updates in the compliance arena, whether internal or external, provide updates on upcoming training opportunities, host confidential reporting outlets (discussed below), and outline any other information that is to be shared throughout the company. Be mindful, however, that this should not be the only avenue for such information. Ensure that materials are available in every medium and in every language necessary to reach all employees.

A note on privilege

How can you best undertake your compliance efforts without diluting the attorney-client privilege and the autonomy of the legal department? Begin by recognizing that the compliance program is going to be used as a shield. To be afforded that protection, it must be structured accordingly.

The compliance work must be clearly distinguished from the legal work. In a department of multiple lawyers, try to vest compliance efforts with a single lawyer, and that work should be treated separately. Implement a file structure that sits outside the legal group where no one else has access other than the compliance team. In addition to clearly defining the compliance roles, this may also alleviate the potential for privilege issues down the road. Retention of privilege will be unequivocal for the legal work, and although the compliance function might be comprised of murkier privilege waters, the focus of that question will be much more narrow.

Policies.

Review all of the policies that your company has on file. We are quick to include the core areas of excellence necessary to drive the business, but other supporting programs can lead to compliance exposures as well. Have you considered policies applicable to all of your subsidiaries and affiliates,

including joint ventures, and all of the parts of the world in which they operate?

Related, consider the last time that each of them were revisited and revised. Are they up to date with recent regulatory changes? Are they reflective of what is happening in the company today, or do they instead reflect the intentions of what should be happening? Do they reflect all acquisitions or expansions of company business? Continuous review is vital — a point discussed in more detail below.

These policies typically reside in HR and company manuals; thus, HR will need to have a fairly prominent seat at the table. Once again, however, they rely largely on the involvement of the subject matter experts to be topical and relevant. The legal department can help foster necessary revisions, and even do the drafting to the extent necessary, but these experts as well as HR should be the primary contributors.

In addition to being published, these policies and procedures manuals should be made available to all employees of the company in a practical way. Having a policy on file won't be sufficient if nobody knows where to find it. Intranet pages are a great way to keep them all in soft copy, but actual hard copies should be available in a conspicuous way. If an employee has a question about the company's OSHA matters, they shouldn't need a treasure map to find the relevant documentation.

Oversight.

Your program must demonstrate an independent reporting structure, periodic reporting, and adequate resources. In practice, this concept is very similar to that of an internal audit — a system of checks and balances ensuring that things are done as they should be done. As mentioned previously, the legal department is not ideally situated within the functional business to accomplish this goal.

If your company has an internal audit department, they may provide some insight. However, similar to the legal department, they have their own independent obligations — be careful not to vest oversight exclusively with that department. Any role they have should be stratified from their day-to-day audit responsibilities much like with legal. If you have no audit department, or if for any other reason oversight responsibility ultimately falls with legal, let it rest with a single lawyer as discussed previously. Even still, that lawyer's role in oversight should be similar to that of the general contractor on a large-scale construction job, outsourcing the responsibilities of functional compliance and conducting an audit of those efforts.

Whether the findings are compiled by audit, legal, or otherwise, they should be delivered to management pursuant to an independent reporting structure that is clearly articulated. This will protect both the integrity of the compliance function as well as the accountability for the participating departments' time. Findings should be reported to management with regularity to keep executive management in the loop on compliance efforts and operational updates. There should be an additional ability, if not an outright obligation, to report the findings independently to the board of directors or the company's audit committee to allow for independent review.

Risk assessments.

Risk assessments are a quantifiable determination of the probability of a loss and the magnitude of loss if it occurs. While a significant number of our colleagues are anti-reading, many lawyers are

equally and oppositely repulsed at the idea of functioning equations within the four corners of an excel spreadsheet.

Surely, conducting a risk assessment does not need to be orchestrated by lawyers; however, assessments require careful thought and planning by people who are capable of appreciating the organization and the regulations applicable to it. Crafting the assessment can be a group effort that should involve legal in the creation of the questions, but quantifying the responses is something that our arithmetically-inclined and risk-identifying cohorts should play a more significant role in presenting. To the extent legal is involved, resist the urge to include broad areas of risk, which can be difficult to calculate and can be overly subjective in nature. Questions should focus on the likelihood of risk and the potential impact if that risk should be realized. Craft the questions so that acthe role of interpretation is minimized. IT may also have some input on the logistics of preparation and distribution (as well as compilation of results) in connection with an assessment.

Thanks to the US Sarbanes-Oxley Act of 2002, if your company is publicly traded, your finance department has likely been operating a comprehensive compliance program since the early 2000s. If your company is privately held, a less-stringent compliance module is required to demonstrate confidence in the financial reports requiring certification by a licensed accountant. They will likely be operating under the structure of the COSO framework, where the financial compliance program is both defined and tested, and will also likely have already planned for compliance shortcomings and other legal obligations by quantifying potential “legal” exposures, which include penalties by regulatory agencies. Your finance group may have advice as to how to structure the compliance program and offer a vocabulary for developing a broader framework to extend enterprise-wide.

Training and continuous advice.

Many companies have dedicated trainers or training teams. Human resources is often involved in this effort, or perhaps subject-matter experts within the business units. Even if the lawyers periodically engage in the training process on isolated topics, this does not mean that legal is steering the ship on this issue.

More often, the lawyers are asked to review training content prior to distribution by others, and perhaps even to assist in the crafting of such content. While that can and should be part of your practice, creating, monitoring, and owning company-wide training efforts is a time-consuming effort that should not belong solely to legal. That said, legal should have an open line of communication with all employees and business lines to provide meaningful advice when and where necessary.

Consider adopting a learning management system to develop and track your training efforts. Automation can take away much of the recordkeeping headache and can prove very valuable in managing the development of your team, both through compliance and other matters. Also worth noting is that these LMS systems generally sit in other departments (IT or HR), further spreading out the obligations of time, effort, and cost.

Consider how training and educational measures are implemented. As noted above, not all employees have access to computers, email, intranet, or other commonly available means of distribution. Be sure that each of your employees receive the same message and educational opportunities. Kiosks for educating and testing are becoming more popular for operations personnel who do not have computers of their own. If language barriers exist in your company, take the appropriate steps to overcome them. Gaps in education and training are the metaphorical equivalent of cracks in the dam: if enough of them exist, the waters of non-compliance can begin to seep

through and your protections can get soggy.

Incentives and disciplinary measures.

Incentives and disciplinary measures, much like all aspects of the compliance program, should be clearly articulated.

Link compliance participation and success to annually-identified goals for all employees. Participation in training sessions, educational opportunities, and successful compliance audits should all yield positive attention within the company. While financial incentives (bonuses, increases, promotions, etc.) are certainly a viable option, even something as simple as regular identification of those units and individuals who meet these goals can be an effective tool.

Regarding discipline, consider the inverse of what has been identified. Failure to meet the identified goals should have meaningful and recognizable impacts. Counseling of individual employees for repeated compliance violations, mandated additional training for sections or business units who fall short, or other (perhaps more draconian) responses can all be levied. On both sides of the spectrum, be sure that these items are being applied reliably, promptly, and uniformly across the business (and at all levels). Responses should be commensurate with the underlying accomplishment/failure.

Responsibility for levying discipline and orchestrating incentive programs for company employees should be almost exclusively the purview of HR. Requisite guidelines may be drafted or co-drafted by legal and should be published to all employees and clearly defined.

Third-party payments/dealings.

When dealing with third parties, particularly internationally, there are a number of obligations of which you should be aware: your customer, export compliance, anti-bribery, supply chain, data security, and social compliance programs should evaluate and track their business partners and the money involved in any deal. Some of this is generated as part of a contractual relationship, where legal may have visibility. Other dealings may be through payments issued within permitted delegations of authority with purchase requisitions, etc., where lawyers may not have visibility.

Lawyers can certainly advise of our organizational obligations, but other departments dealing in these areas will have to implement and maintain their own processes to be compliant. Sales, operations, and various parts of the business should take an active role in the gathering and maintenance of knowledge related to customers and vendors. Legal can provide input and conduct research, perhaps even carrying out background checks or due diligence to ensure compliance, but the decision regarding when and why to carry out these searches should lie with the department conducting the business.

Confidential reporting and internal investigations.

Whistleblower programs have been in existence for some time, however, new scrutiny is being given to the adequacy of those programs. Credit will not be given to organizations that do not have frequent monitoring, independent evaluations of claims, and timely responses to claims.

Proper channels should exist to handle the reporting of potential issues. Confidential email, internet and telephonic “tip lines” can and should be procured through outside vendors to ensure that all

reports are handled in a consistent, timely, and efficient manner by an independent third party. Some companies assemble an internal committee to respond to these complaints to ensure that all issues are being treated with appropriate care, but be aware of the makeup of that committee. While legal may participate, it is likely not best practice for legal to be solely responsible for this function, as this may be the best example of dilution of the attorney/client privilege. When a company attorney becomes intricately involved in the reporting and investigation of issues, particularly those involving allegations against individuals within the company, the clarity of privilege is reduced significantly.

If not on the committee itself, the lawyers should assuredly be apprised of and consulted on certain claims. Legal may even be involved in some of the threshold questions related to these concerns, but ownership of the entire reporting/investigation process is inadvisable.

Continuous improvement.

The compliance program should be constantly evolving and under continuous review. Legal should assist in a significant and meaningful way in this regard. As stewards of the law, we have an obligation to our client to stay continuously informed regarding recent changes and developments in policy. These updates should be shared with the impacted business units to ensure a practical response.

Legal should also advise the compliance team regarding when and if changes to the law require corresponding changes to the program and the underlying policies. Additionally, the department should take a leadership role in the periodic reviews of policies, training, processes, and assessments — even if the underlying modifications aren't carried out solely by legal — to be sure that each of them are representative of current legal trends. A strong relationship between legal and human resources is critical to ensure that underlying policies are revisited and changes are instituted and published on a regular basis.

Also, consider when the compliance work will be carried out. Each area should be regularly monitoring regulatory developments that directly impact their work. As the compliance team meets, verify the team members with expertise in each area and confirm that they are staying informed by credible sources — Bloomberg, OSHA publications, SHRM on employments matters, local digests for updates to the law, other industry-specific publications and updates, etc. Additionally, the responsive alerts received from outside counsel can be incredibly useful tools. These and other summaries of regulatory changes should be circulated through the compliance team on regular mailings for consideration, with the legal department standing at the ready to summarize and answer relevant questions when and where necessary.

Integration of new or divested entities.

The lawyers will of course be involved in corporate M&A transactions, even if only as a conduit to outside counsel, and can prompt an integration program. In putting together such a program, consider how the pieces of your existing compliance program may be impacted by the transaction, and whether any responsibilities need to be shifted or absorbed by a different group within the organization moving forward.

For the newly acquired entity, consider how to roll them into your existing program. Lawyers will need to be working closely with the business team so compliance matters of the target entity, including open investigations or other impactful disclosures, are a recognized economic factor that is

considered in the transaction prior to closing. Penalties for non-compliance may be too large to ignore and can erode any potential gains of a solid commercial transaction.

The business team should understand and appreciate this exposure early and often. The preparation of disclosure schedules and an appreciation for what's on them, while typically reserved for the slow and torturous education of junior M&A associates, should be the responsibility of the entire deal team including the business. However, rest assured that if an issue exists on the schedule that isn't properly vetted prior to closing, the first questions to be asked will be of the legal department.

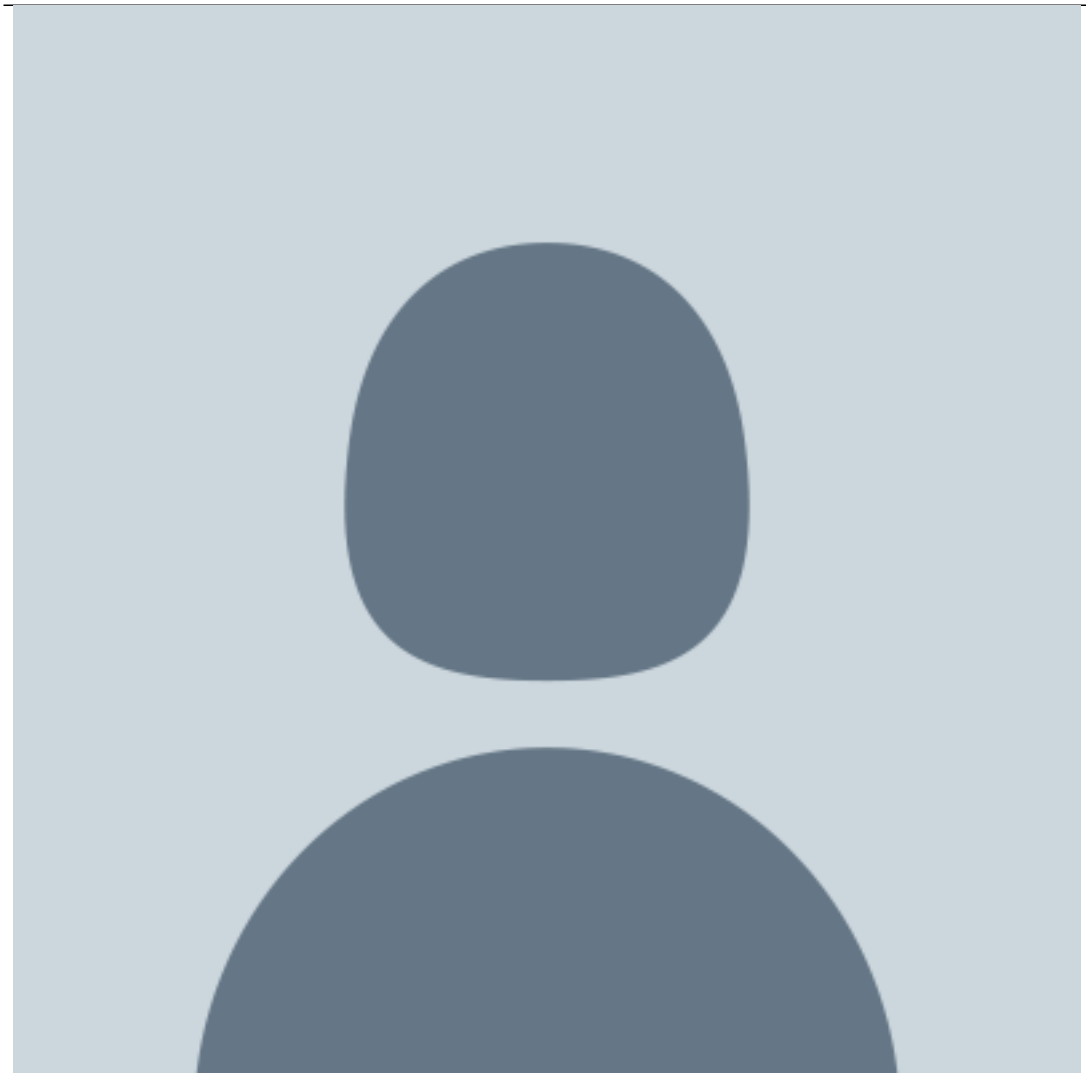
While these Ten Hallmarks reflect some of the guiding principles of a successful program, consider that there are compliance conventions that can and should be utilized as the lens through which you view your compliance efforts. The earlier-referenced COSO model is one such method that may be utilized internationally. In addition, there may be a variation to adapt to the internationally-recognized ISO conventions (such as AS/ISO 19600:2015 (AS/ISO 19600). Your audit team will also likely be familiar with the COSO methodology and can offer advice in structuring the program and adapting the financial modeling tools to compliance concepts rather quickly.

Additionally, if you are an international company and ISO certified, you may want to consider a structure that draws from the ISO 31000 risk management guidance. This standard is internationally recognized and may offer credible basis and approach in developing or refining the compliance team approach.

COSO and ISO are two widely-recognized modeling and compliance structures that will not only add significant credibility to your program, but will also maximize your resources and provide an additional layer of meaningful defense if regulators should become interested in your company's program.

So while it's clear that legal will clearly play a role — and perhaps a significant one — in a robust and successful compliance program, the rest of the company should share in the burden, rather significantly in some cases. You should identify someone within each of the departments referenced above to be appointed to your newly-minted compliance committee. That person should have firsthand knowledge of their topic area, and should also have the decision-making authority (or access to someone who does) within that department, so that change can be implemented where necessary. Remember that the lawyer's voice at the table is simply to educate on what should be happening. The other, more operationally focused voices within your company, are the voices that can report on what is happening. Listening to both is what will optimize your compliance efforts and provide the best support and protection for your company.

Stephanie Bortnyk



a Director and Associate General Counsel

Dassault Falcon Jet Corp

She supports all areas of the business, including negotiations and advice related to aircraft sales, procurement efforts, general business matters, and industry-specific laws and regulations.

Carl J. Peterson

General Counsel

Mid-Atlantic Business Unit at Titan America LLC